8MAN

DER IT-GRUNDSCHUTZ-KATALOG IM FOKUS

Mit 8MAN Anforderungen des BSI umsetzen.

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) vertritt mit dem Grundschutz-katalog eine Reihe von Anforderungen für den sicheren Betrieb von IT-Systemen. Darin enthalten sind technische, organisatorische, personelle und infrastrukturelle Maßnahmen, die für die Absicherung von IT-Systemen relevant sind. Als zentrale Zertifizierungsstelle für IT-Sicherheit in Deutschland legt das BSI ein besonderes Augenmerk auf die Verwaltung von Zugriffsrechten.

Als Marktführer im Bereich Access Rights Management sind die Empfehlungen des BSI ein zentraler Maßstab für die Weiterentwicklung unserer Lösung. 8MAN erfüllt einen großen Teil der BSI Anforderungen und geht in Teilen sogar noch darüber hinaus.

Das vorliegende Dokument zeigt unsere Lösung zu jeder der vom BSI genannten Maßnahmen. Da unser Produkt feingranular strukturiert ist, sind wir in der Lage, zu jeder BSI Prüffrage den korrespondierenden 8MAN Service zu zeigen. Über die eingefügten Links gelangen Sie direkt
in unsere Online-Hilfe, in der unser gesamtes Funktionsspektrum dokumentiert ist.

Anhand der in jeder Maßnahme gestellten „Prüffragen" können Sie einerseits den Professionalisierungsgrad Ihrer IT bestimmen und andererseits prüfen, wie 8MAN bei der Umsetzung zentraler BSI Anforderungen behilflich ist.

Wir wünschen Ihnen viel Spaß bei der Umsetzung der BSI Anforderungen. Sollten Sie für die Optimierung Ihrer IT professionelle Unterstützung benötigen, sind wir jederzeit für Sie da.

Stephan Brack, CEO **Sven Reinhardt,** CTO **Matthias Schulte-Huxel,** CSO

Inhaltsverzeichnis

Zur 15. Ergänzungslieferung für den BSI Grundschutzkatalog

Mit der 15. Ergänzungslieferung für den IT-Grundschutzkatalog hat das BSI ein neues Anforderungspaket definiert. Im **Baustein Identitäts- und Berechtigungsmanagement** sind alle Prozesse und Maßnahmenpakete enthalten, die für eine sichere IT relevant sind.

Der Baustein gliedert sich in vier Bereiche: Planung und Konzeption, Beschaffung, Umsetzung und Betrieb. Innerhalb dieser Bereiche sind Maßnahmen definiert. Diese werden im Rahmen dieses Dokumentes kurz skizziert. Anhand der Prüffragen bestimmen Sie den Reifegrad Ihrer IT.

8MAN bietet darüber hinaus noch weitere Services, die abseits des Themenclusters „Identitäts- und Berechtigungsmanagement" vom BSI gefordert werden. Sie finden diese aufgelistet im zweiten Teil dieses Dokumentes. 8MAN geht damit die Extrameile im Access Rights Management. Nicht nur die Zugriffsrechte sind dabei im Fokus, sondern auch die korrespondierenden Aktivitäten und Prozesse.

Alle Angaben beziehen sich sowohl auf ein Active Directory & Fileserver. Fragen Sie unseren Vertrieb für die Analyse weiterer Ressourcen.

BSI: Alle mit diesem Symbol markierten Überschriften und Textpassagen verlinken direkt in den BSI Online Katalog und beschreiben die jeweiligen Katalognummern ausführlich.

Help: Alle mit diesem Symbol markierten Links verlinken in das 8MAN Manual und beschreiben den jeweiligen Service näher. Gleichzeitig werden anhand von Screenshots auch Empfehlungen zur Konfiguration gegeben.

Das IT-Sicherheitskonzept von 8MAN

Mit insgesamt acht Disziplinen verfügt 8MAN über das größte Leistungsportfolio auf dem Markt.

Die fünf Kerndisziplinen bilden in ihrer Gesamtheit ein klares und schnell zu implementierendes System für eine professionelle Zugriffsrechteverwaltung in Ihrem Unternehmen.

Zentral für die Absicherung Ihrer Daten ist **Permission Analysis.** 8MAN zeigt die Berechtigungssituation in Ihrem Netzwerk bidirektional: Entweder wählen Sie eine sicherheitskritische Ressource und lassen sich anzeigen, wer darauf Zugriff hat, oder Sie lassen sich die Zugriffsrechte eines Nutzers anzeigen.

Documentation & Reporting schafft eine klare Dokumentation der Zugriffsrechte. Alle mit 8MAN vergebenen oder entzogenen Rechte sind im Logbuch erfasst und können in verständlichen Reporten dargestellt werden. Sie erkennen sofort, wer welche Rechte an wen vergeben hat. Bei sicherheitsrelevanten Aktionen verlangt 8MAN immer die Eingabe eines Kommentars. Mit einer kurzen Begründung oder Ticketnummer ist auch nach langer Zeit nachvollziehbar, weshalb ein Zugriffsrecht geändert wurde.

Mit dem **Security Monitoring** vertiefen Sie das Sicherheitsniveau und erfassen auch Aktivitäten, die außerhalb von 8MAN vorgenommen wurden. Sollte sich ein Mitarbeiter mit Bordmitteln Einblick in geschützte Verzeichnisse verschaffen, löst 8MAN sofort einen Alarm aus. Dateizugriffe, Manipulationen am AD und Eingriffe an ausgewählten Postfächern werden lückenlos dokumentiert.

Zugriffsrechte regeln die Verteilung von Firmenwissen. Sie sind geschäftskritisch und sollten nicht vom Administrator vergeben werden. Mit **Role & Process Optimization** wird die Verwaltung von Zugriffsrechten zu einem optimierten Business-Prozess. Data Owner (Führungskräfte) ordnen die Zugriffsrechte ihren Mitarbeitern zu. Diese wissen im Gegensatz zum Administrator, welche die schützenswerten Informationen in der Abteilung sind und wer darauf Zugriff haben sollte. Über individuell definierbare Freigabe-Workflows ist die Verantwortung eindeutig geklärt.

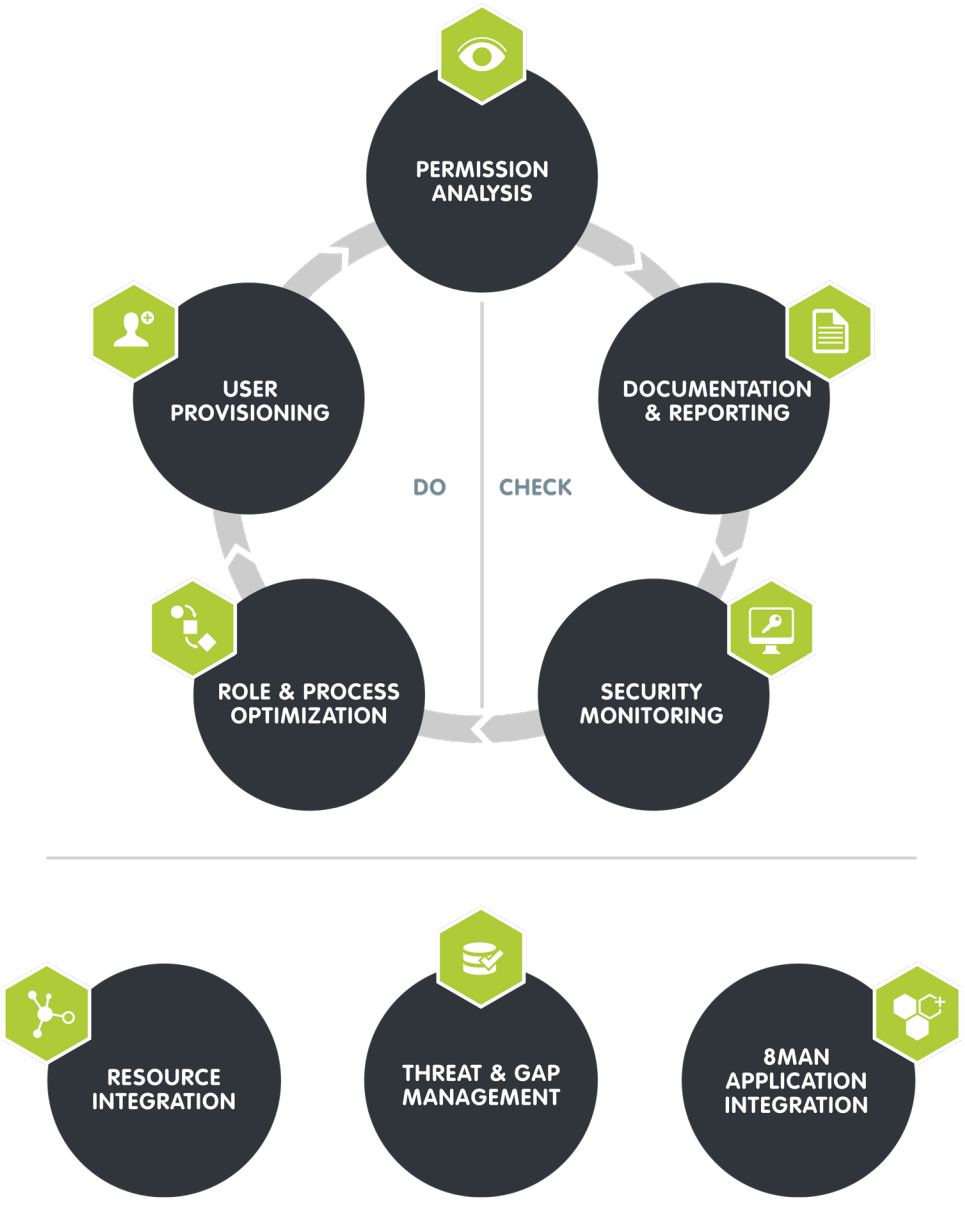
Die geregelte Vergabe und der Entzug von Zugriffsrechten scheitern häufig an der Effizienzhürde. Genau an dieser Stelle setzt **User Provisioning** an: Nutzerkonten und ihre Zugriffsrechte können auch durch nicht IT-versierte Business Units schnell und einfach verändert werden.

Ein ganzheitliches Berechtigungsmanagement darf sich nicht allein auf die Zugriffsrechte im Active Directory und in Fileservern beschränken. Mit **Resource Integration** folgen wir unserer Vision, immer mehr berechtigungsabhängige Anwendungen in die 8MAN Lösung zu integrieren. Unser Ziel ist eine Oberfläche, mit der Sie alle Anwendungen analysieren und administrieren können. Neben den Basistechnologien Active Directory und Fileserver haben wir MS Exchange, MS SharePoint und MS Dynamics NAV erfolgreich eingebunden. Mit unserer offenen Schnittstelle "Easy Connect" können Sie auch selbst Daten in 8MAN einlesen. Sie gewinnen so die 8MAN-typische Übersicht über die Berechtigungslage weiterer Systeme.

Die Korrektur von Berechtigungsfehlern und Inkonsistenzen ist auf Fileservern nur schwer möglich. Die Umsetzung von Best Practices scheitert an zwei zentralen Hürden: Wissen und Zeit. Darüber hinaus liegt der Fokus im klassischen Access Rights Management (ARM) auf der Verzeichnisebene. Sie ist die zentrale Analyseebene, blendet aber die Dateiebene aus. **Threat & Gap Management** startet einen Prozess, der in einen sicheren und standardisierten Fileserver mündet. Durch eine Reihe klarer Entscheidungen definieren Sie, wie mit Sicherheits- und Strukturproblemen umgegangen werden soll. Ihre Anforderungen und die in 8MAN hinterlegten Best Practices werden automatisch umgesetzt. Darüber hinaus ist die Archivierung veralteter Daten möglich. Denn: je geringer die Dateimasse, desto einfacher die Verwaltung.

Moderne IT-Lösungen müssen in der Softwarelandschaft einer strukturierten IT miteinander vernetzt sein. Insellösungen schaffen Frustration bei Nutzern, Administratoren und IT-Leitern. **8MAN Application Integration** ist die serienmäßig enthaltene WebAPI. Diese lässt sich für die Anbindung an zahlreiche Lösungen nutzen.

Disziplinen für systematisches Access Rights Management



Katalognummer: M 2.5 Aufgabenverteilung und Funktionstrennung

Die Maßnahme fordert u.a., die Rechteverwaltung und die Revision personell voneinander zu trennen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind alle relevanten Funktionen innerhalb der Institution definiert, die Informationen zu ihrer Aufgabenerfüllung verwenden oder dabei unterstützend tätig sind?	Die Protected Networks GmbH bietet Ihnen im Rahmen unserer Professional Services eine fachgerechte und maßgeschneiderte Implementierung von 8MAN. Zentral ist dabei die Erstellung eines maßgeschneiderten Rollenkonzeptes für Ihre Firma und dessen Abbildung in der Nutzerverwaltung von 8MAN.
Sind Funktionstrennungen für unvereinbare Funktionen vollständig festgelegt und dokumentiert?	Mit 8MAN involvieren Sie Auditoren und Datenschützer über zwei Möglichkeiten in Ihre Sicherheitsprozesse: - Sie geben der Person einen einfachen Lesezugriff in 8MAN. - Sie definieren zusammen, welche Reporte interessant sind, und 8MAN versendet diese automatisch im vereinbarten Turnus. **Weiterführende Infos:** → einer Sicherheitrolle die Analyse der Berechtigungs-situation ermöglichen
Wird die Funktionstrennung personell aufrechterhalten?	N/A

Katalognummer: M 2.11 Regelung des Passwortgebrauches

Die Maßnahme empfiehlt Regeln für den korrekten Gebrauch von Kennwörter. Neben dem Verzicht auf Trivialpasswörtern sind vor allem die regelmäßigen Änderungen der Passwörter eine zentrale Anforderung des BSI.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Gibt es eine verbindliche Regelung für den Passwortgebrauch?	N/A
Sind die Benutzer angewiesen, Passwörter mit ausreichender Komplexität zu verwenden, die dem Schutzbedarf angemessen sind?	8MAN überprüft beim Anlegen neuer Benutzer die in der Domäne festgeschriebene Passwort-Policy.
Sind die Benutzer angewiesen, ihr Passwort geheim zu halten?	N/A
Wird getestet, wie viele Stellen des Passwortes tatsächlich vom IT-System überprüft werden?	N/A
Werden Passwörter in regelmäßigen Abständen gewechselt?	**User Provisioning** → Kennwortoptionen eines Benutzers ändern → Kennwortoptionen im Bulk ändern → Benutzer mit nie ablaufenden Kennwörtern identifizieren **Security Monitoring** → Kennwortrücksetzungen überwachen
Werden Passwörter sofort gewechselt, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht?	**User Provisioning** → Ein Kennwort zurücksetzen → Kennwörter im Bulk zurücksetzen **Ab Release 9.0:** → Das Kennwort eines Mitarbeiters ändern
Bei erfolglosen Anmeldeversuchen: Wird nicht bekannt gegeben, ob Benutzername und/oder Passwort falsch waren?	N/A

Katalognummer: M 2.30 Regelung für die Einrichtung von Benutzern/Benutzergruppen

Das BSI fordert eine geordnete Einrichtung von Benutzern und Benutzergruppen.
Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Rechtevergaben, die über den Standard hinausgehen, müssen dokumentiert und begründet werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Bei zusätzlichen Zugriffsberechtigungen, die über das Standardprofil hinausgehen: Werden diese nur nach zusätzlicher Begründung vergeben?	**User Provisioning** 8MAN dokumentiert alle Änderungen automatisch. Der Ausführer muss seine Aktionen immer kommentieren. **Documentation & Reporting** → Access Rights Management Aktivitäten berichten
Gibt es eine geregelte Vorgehensweise zur Einrichtung von Benutzern und Benutzergruppen?	→ Die Nutzeranlage mit Templates standardisieren → Ein Nutzerkonto anlegen → Gruppen anlegen und Benutzer hinzufügen → Gruppenmitgliedschaften bearbeiten
Existiert eine separate administrative Rolle für das Einrichten von Rechten bzw. Rechteprofilen?	In 8MAN lässt sich die Fähigkeit der Einrichtung einer Rolle im User Management definieren.

Katalognummer: M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle

Das BSI empfiehlt, Standard-Rechteprofile für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben festzulegen. Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen, abhängig von der jeweiligen Rolle, dem Need-to-Know-Prinzip folgen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Existieren dem Schutzbedarf der Organisation angemessene Regelungen zur Zugangs- und Zugriffskontrolle?	N/A
Existieren Standard-Rechteprofile, die den Funktionen und Aufgaben der Nutzer entsprechen?	**User Provisioning** Mit Release 9.0 bietet 8MAN Profile. Diese verfügen über einen abteilungsspezifischen Basissatz an Berechtigungen. Damit ist die Implementierung eines Berechtigungskonzeptes schnell möglich. → Ein neues Abteilungsprofil erstellen
Existieren schriftliche Zugriffsregelungen sowie eine Dokumentation der Benutzereinrichtung und der Rechtevergabe?	**Documentation & Reporting** 8MAN verfügt über eine Reihe von Reporten, die sowohl die Benutzereinrichtung als auch die Rechtevergabe dokumentieren: → Wo haben Benutzer/Gruppen Zugriff? **Security Monitoring** → Änderungen im Active Directory überwachen
Wird der Zugriff auf alle IT-Systeme und Dienste durch Identifikation und Authentikation des zugreifenden Benutzers oder IT-Systems abgesichert?	N/A
Werden Authentisierungsdaten erst nach vollständiger Eingabe überprüft?	8MAN überprüft die Authentisierungsdaten erst nach vollständiger Eingabe.

Katalognummer: M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements

Das BSI fordert die Erstellung und Umsetzung eines Berechtigungskonzeptes. Zentral darin sind Richtlinien sowie Trennung der Funktionen und Rollen. Darüber hinaus wird ein geregeltes Verfahren beim Anlegen, ändern und löschen von Berechtigungen gefordert.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist festgelegt worden, wer welche Aufgaben und Zuständigkeiten im Rahmen des Identitäts- und Berechtigungsmanagements hat?	**Role & Process Optimization** → Delegation von Aufgaben im Access Rights Management
Existiert ein Konzept für das Identitätsund Berechtigungsmanagement?	**User Provisioning** Mit Release 9.0 bietet 8MAN Profile. Diese verfügen über einen abteilungsspezifischen Basissatz an Berechtigungen. Damit ist die Implementierung eines Berechtigungskonzeptes schnell möglich. → Ein neues Abteilungsprofil erstellen (Administrator) → Ein neues Abteilungsprofil zuweisen (Cockpit)

Katalognummer: M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen

Das BSI fordert die zentrale Verwaltung von Zugriffsrechten und empfiehlt die Verwendung von Benutzer- und Rechtemanagementwerkzeugen, um den Administrations und Pflegeaufwand zu reduzieren.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Werden alle Benutzerkennungen und Berechtigungen ausschließlich auf Basis des tatsächlichen Bedarfs vergeben?	8MAN propagiert ein zweistufiges Berechtigungssystem. Über ein Abteilungsprofil erhält der Mitarbeiter die grundlegenden Rechte, die er benötigt. Die zusätzlichen Rechte bestellt der Mitarbeiter über das 8MATE GrantMA Self-Service-Portal. Je nach Konfiguration entscheidet der Administrator, die zuständige Führungskraft oder es entscheiden beide über die Freigabe. **Role & Process Optimization** → Als Mitarbeiter Fileserverrechte bestellen → Als Administrator oder Führungskraft eine Anfrage ablehnen oder bestätigen In einem regelmäßigen Rezertifizierungsworkflow prüfen die Führungskräfte in den Fachabteilungen die Zugriffsrechtesituation und passen diese in einem einfachen Workflow an. → Bestehende Zugriffsrechte rezertifizieren
Werden bei personellen Veränderungen die nicht mehr benötigten Benutzerkennungen und Berechtigungen unbrauchbar gemacht?	Mit 8MAN kann entweder die Führungskraft oder der Administrator ein Nutzerkonto sofort sperren. Damit ist der Zugriff auf das System nicht mehr möglich. → Einen Benutzer sperren Der Administrator entfernt das Nutzerkonto und die Berechtigungen in einem Zug. → Einen Nutzer und seine Berechtigungen löschen
Werden die vorgenommenen Berechtigungsänderungen dokumentiert?	8MAN dokumentiert alle Änderungen automatisch. Der Ausführer muss seine Aktionen immer kommentieren. **Documentation & Reporting** → Access Rights Management Aktivitäten berichten

Katalognummer: M 2.587 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement

Die Richtlinie für das Identitäts- und Berechtigungsmanagement beschreibt die folgenden Teilprozesse:

- Identitätsprofile verwalten
- Berechtigungsprofile verwalten
- Benutzerkennungen verwalten
- Rollen verwalten
- Analyse von Identitäten und Berechtigungen und Konten verwalten

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Keine Prüffragen vorhanden.	**User Provisioning** 8MAN steuert den gesamten Nutzerkonto-Lifecycle (Joiner-, Mover-, Leaver-Prozess). Ein Nutzerkonto wird mit einem Template bzw. Profil angelegt. Mit einem Abteilungsprofil wird ein Basissatz an Berechtigungen zugewiesen. In der Fachabteilung werden spezielle Berechtigungen vergeben. Bei Austritt aus dem Unternehmen werden alle Rechte kontrolliert entzogen und das Nutzerkonto wird deaktiviert.

Katalognummer: M 4.133 Geeignete Auswahl von Authentikationsmechanismen

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist sichergestellt, dass jede weitere Interaktion mit dem System oder der Anwendung erst nach erfolgreicher Identifikation und Authentisierung möglich ist?	8MAN ist nur passwortgeschützt zu erreichen. 8MAN lässt sich mit Hilfe eines Servicekontos zum führenden System im Active Directory machen. Eine Arbeit mit Bordmitteln ist dann nicht mehr möglich und das AD ist vor sonstiger Manipulation geschützt.
Kommen dem Schutzbedarf entsprechend angemessene Identifikations- und Authentisierungsmechanismen zum Einsatz?	8MAN Passwortschutz.
Können Authentisierungsdaten für Benutzer ausschließlich von autorisierten Administratoren angelegt bzw. verändert werden?	Im Rollenmodell von 8MAN können nur der Administrator oder Help Desk Authentisierungsdaten ändern und Konfigurationseinstellungen vornehmen
Werden die Authentisierungsdaten durch das IT-System bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt?	Die Authentisierungsdaten sind nach Advanced Encryption Standard (AES) geschützt. Die Daten werden nur im konkreten Anwendungsfall aufgerufen.
Können die eingesetzten Authentisierungsmechanismen Anmeldevorgänge nach einer vorgegebenen Anzahl von Fehlversuchen beenden?	Ja, dabei wirken die Einstellungen in der Active Directory Password Policy. Wir empfehlen, diese restriktiv zu gestalten.
Werden abgelaufene Benutzerkennungen automatisch gesperrt?	8MAN zeigt das Kontoablaufdatum und den Kennwortablauf in einem Report: → Benutzer-und-Gruppen-Report → Nicht mehr verwendete Nutzerkonten zeigt der Inaktive-Konten-Report
Werden Authentisierungsvorgänge in einem für die Institution angemessenen Umfang protokolliert?	N/A

Katalognummer: M 4.250 Auswahl eines zentralen, netzbasierten Authentisierungsdienstes

Nach dem BSI sollten IT-Systeme aller Art grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen.
Nur so kann verhindert werden, dass unautorisierte Personen Zugriff auf die Dienste erlangen, die das System anbietet, oder auf die Daten, die auf dem System gespeichert sind.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurde im Einsatz von eines zentralen, netzbasierten Authentisierungsdienst der Einsatz sorgfältig geplant?	N/A
Wurden die für die Auswahl eines zentralen, netzbasierten Authentisierungsdienstes relevanten Sicherheitsanforderungen dokumentiert?	N/A

Katalognummer: M 4.498 Sicherer Einsatz von Single Sign-On

Single Sign On ermöglicht Administratoren die einfachere Verwaltung von Identitäten und Berechtigungen. Nutzer profitieren von der einmaligen Anmeldung. Aus Sicherheitssicht bringt ein SSO daher viele Vorteile, aber auch einige Risiken. Das BSI stellt diesbezüglich Kriterien auf.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Entsprechen die bei Single Sign-On genutzten Sicherheitsmechanismen den Anforderungen der angeschlossenen Anwendungen bzw. Systeme?	Der Webclient ist über SSO erreichbar.
Wird bei SSO konsequent eine Zwei-Faktor-Authentisierung genutzt?	N/A
Werden Authentisierungsinformationen bei SSO ausschließlich verschlüsselt übertragen und gespeichert?	Ja, die Übertragung erfolgt stets verschlüsselt.

Katalognummer: M 5.34 Einsatz von Einmalpasswörtern

Passwörter können in Netzwerken relativ einfach abgehört werden. Deshalb fordert das BSI den Einsatz von Einmalpasswörtern und die Verschlüsselung ebendieser.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist sichergestellt, dass keine wiederverwendbaren Passwörter unverschlüsselt über das Netz übertragen werden?	Die Passwörter werden innerhalb von 8MAN durch Advanced Encryption Service (AES) verschlüsselt. Mit 8MAN kann die Führungskraft das Kennwort eines Mitarbeiters zurücksetzen. Die Übergabe des Einmalpasswortes erfolgt dann direkt an den Mitarbeiter.

Katalognummer: M 4.499 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen

Das BSI rät zum Einsatz eines Identitäts- und Berechtigungsmanagement- Systems.
Für die Auswahl einer geeigneten Lösung referenziert das BSI auf eine Reihe von Prüfkriterien.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Kann der Grundsatz der Funktionstrennung realisiert werden (M 2.5 Aufgabenverteilung und Funktionstrennung)?	8MAN hat eine eigene Benutzerverwaltung und erlaubt die Konstruktion klarer Rollen und Funktionen. → Benutzer verwalten
Interoperabilität: Ist das Identitäts- und Berechtigungsmanagement-System in der Lage, die unterschiedliche Berechtigungsverwaltung heterogener Anwendungen zentral zu integrieren?	8MAN integriert standardmäßig die Verwaltung von Active Directory- und Fileserverressourcen. Darüber hinaus lassen sich Microsoft SharePoint, Exchange und Dynamics NAV integrieren. Mit unserem „Easy Connect" sind Sie in der Lage, beliebige Ressourcen über einen CSV-Import zu integrieren. → 8MAN Resource Integration
Unterstützt die Anwendung den Einsatz der geplanten Authentisierungsfaktoren Wissen, Besitz bzw. Biometrie?	N/A
Ist eine Skalierung der Authentisierungsanforderungen je nach Schutzbedarf möglich?	8MAN erlaubt, für besonders sicherheitskritische Verzeichnisse spezifische Credentials zu definieren. Damit ist der Schutzbedarf skaliert.
Sind durchgängige Rechteänderungen bis hin zum Rechteentzug kurzfristig möglich, wenn diese akut benötigt wird (z. B. Mitarbeiter wird fristlos freigesetzt)?	Mit 8MAN können wahlweise der Administrator, die zuständige Führungskraft oder die Personalabteilung Rechte entziehen bzw. das Nutzerkonto sperren.
Werden Authentisierungsdaten bei Speicherung und Verarbeitung ausreichend geschützt (nicht als Klartext, sondern stets verschlüsselt gespeichert bzw. übertragen)?	Ja, alle Authentisierungsdaten werden stets verschlüsselt übertragen.
Entsprechen die im Identitäts- und Berechtigungsmanagement-System vorhandenen kryptografischen Funktionen dem Schutzbedarf und besitzen sie eine ausreichende Mechanismenstärke (siehe auch M 2.164 Auswahl eines geeigneten kryptografischen Verfahrens)?	Die vorhandenen kryptografischen Verfahren basieren auf dem Advanced Encryption Service (AES), einem zeitgemäßen Kryptografieansatz.
Werden die Authentisierungsdaten sicher verwaltet?	Die Daten befinden sich in verschlüsselter Form in einer Datenbank.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist sichergestellt, dass beispielsweise Passwörter nie unverschlüsselt auf den entsprechenden IT-Systemen gespeichert werden?	Ja, über den AES.
Wie schnell können die Identitäten, Berechtigungen oder Passwörter geändert werden, z. B. bei Verdacht auf Kompromittierung?	Im Falle eines Sicherheitsvorfalls setzen Sie befallene Konten mit 8MAN im Bulk zurück. → Nutzerkonten im Bulk zurücksetzen
Kann die Reaktion auf fehlerhafte Authentisierungsversuche entsprechend den Sicherheitsvorgaben eingerichtet werden?	Ja, dabei wirken die Einstellungen in der Active Directory Password Policy.
Lassen sich die sicherheitskritischen Parameter wie Authentisierungsanforderungen entsprechend den Sicherheitsvorgaben konfigurieren?	Das geschieht im Verzeichnisdienst (Active Directory).
Lassen sich auf dem Identitäts- und Berechtigungsmanagement-System differenzierte Rechtestrukturen in zugewiesenen Bereichen für das Verwaltungspersonal einrichten (lesen, schreiben, ausführen, ändern)?	8MAN erlaubt die Erstellung von sehr differenzierten Rechtestrukturen. Auch nicht IT-affine Führungskräfte können geschützte Bereiche anlegen. **User Provisioning** → Einen geschützten Fileserverbereich anlegen
Sind die Protokolle selbst für Unberechtigte weder lesbar noch modifizierbar? Ist die Protokollierung übersichtlich, vollständig und korrekt? Verfügt das Identitäts- und Berechtigungsmanagement-System über eine übersichtliche und einfach nutzbare Protokollauswertung? Verfügt das Identitäts- und Berechtigungsmanagement-System über eine angemessene Protokollierung?	8MAN hat eine umfassende Protokollierung. Diese ist im Logbuch abrufbar. Wer darauf Zugriff hat, regelt der Administrator in der 8MAN Benutzerverwaltung. Das Logbuch ist für keine Rolle modifizierbar. **Documentation & Reporting** → Logbuch Report
Werden die für die Rechteverwaltung relevanten Daten manipulationssicher vom Produkt gespeichert?	Die Datenbank muss vom Endkunden über das Betriebssystem vor unberechtigtem Zugriff geschützt werden.
Ist sichergestellt, dass die Protokollierung von Unberechtigten nicht deaktiviert werden kann?	Die 8MAN Konfiguration ist durch ein Kennwort geschützt.

Katalognummer: M 1.1 Einhaltung einschlägiger Normen und Vorschriften

Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für die Benutzer und an Sicherheit für den Betrieb gewährleisten. Auch für den Bereich Identity und Access Management fordert das BSI die Überprüfung der Einhaltung der Vorschriften.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Werden alle relevanten Normen und Vorschriften bei Planung, Errichtung und Umbau von Gebäuden sowie dem Einbau von technischen Einrichtungen berücksichtigt?	N/A

Katalognummer: M 2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen

Nach dem BSI muss Klarheit darüber bestehen, wie sich Benutzer vor dem Zugriff auf die mit der Anwendung verarbeiteten Daten authentisieren.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurden die Anforderungen an Funktion und Sicherheit der Authentisierung geeignet umgesetzt?	8MAN verfügt über eine eigene Benutzerverwaltung. Darin lässt sich jede Anwenderrolle feingranular definieren. Für den Webclient ist SSO möglich.
Ist die Speicherung und Übermittlung von Authentisierungsinformationen kryptografisch ausreichend abgesichert?	Ja, dabei kommt der Advanced Encryption Standard zum Einsatz.

Katalognummer: M 4.1 Passwortschutz für IT-Systeme

Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist sichergestellt, dass nur berechtigte Personen auf Anwendungen und IT-Systeme zugreifen können?	8MAN ist nur über die Eingabe eines Passwortes zu erreichen. Der Webclient funktioniert über Single Sign-On.

Katalognummer: M 4.7 Änderung voreingestellter Passwörter

Das BSI fordert, voreingestellte Passwörter spätestens bei erstmaliger Inbetriebnahme zu ändern.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Werden Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert, bevor IT-Systeme in Betrieb genommen werden?	**User Provisioning** Mit der Checkbox „Benutzer muss Passwort vor dem ersten Gebrauch ändern" gewährleistet 8MAN, dass der Nutzer sein Passwort individualisiert. **User Provisioning** → Kennwortoptionen eines Benutzers ändern → Kennwortoptionen im Bulk ändern
Wird überprüft, ob tatsächlich kein Systemzugang mit Standardpasswörtern oder schwachen Passwörtern möglich ist?	N/A

Katalognummer: M 2.6 Vergabe von Zutrittsberechtigungen

Das BSI fordert die kontrollierte Vergabe von Berechtigungen zum Zutritt zu schutzbedürftigen Räumen für Personen. Der Schutzbedarf eines Raumes leitet sich ab aus dem Schutzbedarf der im jeweiligen Raum verarbeiteten Informationen, der dort vorhandenen IT-Systeme und der Datenträger, die in diesem Raum gelagert und benutzt werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktionen vergeben wurden?	**Documentation & Reporting** Wird der Zugang zu Räumen über ADGruppen gewährleistet, hilft 8MAN mit Purpose Groups: Geben Sie den Funktionsgruppen aussagekräftige Namen, z. B. „Serverraum". Damit ist eine eindeutige Zuweisung von Zutrittsrechten möglich. **Purpose Groups: Gruppen bezeichnen**
Ist die Dokumentation der Zutrittsberechtigungen aktuell und vollständig in Bezug auf schutzbedürftige Räume?	**Documentation & Reporting** Mit unserem Kontodetailsreport können Sie alle Purpose Groups auflisten und die zutrittsberechtigten Personen für die jeweiligen Räume identifizieren. → Kontodetails-Report

Katalognummer: M 2.7 Vergabe von Zugangsberechtigungen

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. Systemkomponenten und Netze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Orientiert sich die Vergabe von Zugangsberechtigungen an den Funktionen der Zugangsberechtigten?	**User Provisioning** Mit Release 9.0 bietet 8MAN Profile. Diese verfügen über einen abteilungsspezifischen Basissatz an Zugangsberechtigungen. **Role & Process Optimization** Die feingranulare Zuweisung von Zugangsrechten erfolgt über den Mitarbeiter-Data-Owner-Workflow. Der Mitarbeiter bestellt Zugang zu einer Applikation (via AD Gruppe) und der Vorgesetzte entscheidet über die Bewilligung. 8MAN führt die Prozesse automatisch im Hintergrund aus.
Liegt eine aktuelle Dokumentation über die Vergabe sowie den Entzug von Zugangsberechtigungen und Zugangsmitteln vor?	**Documentation & Reporting** 8MAN zeigt bereits mit einem Mouseover für jedes Nutzerkonto die letzten Aktivitäten an. Alternativ sehen Sie diese feingranular im folgenden Report aufgelistet: → 8MAN Access Rights Management Aktivitäten erfassen (Logbuch Report)
Werden die Zugangsberechtigten auf den korrekten Umgang mit Zugangsmitteln hingewiesen?	N/A
Werden Zugangsberechtigungen bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt?	**User Provisioning** Mit dem Release 9.0 wird es für Administratoren und Führungskräfte möglich, Nutzerkonten und damit die Zugangsberechtigungen für definierte Zeiträume zu sperren.

Katalognummer: M 2.8 Vergabe von Zugriffsrechten

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, ITAnwendungen oder Daten zu nutzen. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (Need-to-know-Prinzip).

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?	**Documentation & Reporting** Folgende Reporte helfen bei der Kontrolle: → Wer hat wo Zugriff? → Wo haben Mitarbeiter eines Managers Zugriff? → Wo haben Benutzer und Gruppen Zugriff? → Wer kann wo über welche Berechtigungsgruppen zugreifen? → 8MAN Access Rights Management Aktivitäten erfassen (Logbuch Report)
Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?	**Permission Analysis** Die folgenden Services schaffen Klarheit. → Überberechtigte Benutzer anhand des Kerberos Tokens identifizieren → Ein Verzeichnis und die Berechtigungen darauf identifizieren → Einen Benutzer und seine Berechtigungen identifizieren → Mehrfachberechtigungen auf Verzeichnissen identifizieren
Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?	**Role & Process Optimization** → Die Verzeichnisrechte Verwaltung an einen Data Owner (Führungskraft) delegieren → Freigabe-Workflows definieren → FS-Zugriffsrechte beim Data Owner bestellen
Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?	**Role & Process Optimization** → Bestehende Zugriffsrechte rezertifizieren **User Provisioning** → Gruppenmitgliedschaften bearbeiten → Einen Nutzer und seine Berechtigungen löschen → Einen Nutzer mittels „Soft Delete" löschen

Katalognummer: M 2.22 Hinterlegen des Passwortes

Ist der Zugriff auf ein IT-System durch ein Passwort geschützt, so müssen Vorkehrungen getroffen werden, die bei Abwesenheit eines Mitarbeiters, z. B. im Urlaubs- oder Krankheitsfall, seinem Vertreter den Zugriff auf das IT-System ermöglichen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Ist sichergestellt, dass benannte Vertreter auf die benötigten Anwendungen und IT-Systeme zugreifen können?	N/A
Ist geregelt, welche Passwörter hinterlegt werden müssen und welche Sicherheitsvorkehrungen dabei einzuhalten sind?	N/A
Werden Passwörter nur dann hinterlegt, wenn es keine andere zweckmäßige Vorgehensweise gibt, die notwendigen Zugriffsmöglichkeiten zu schaffen?	N/A
Wenn Passwörter hinterlegt werden: Werden die Passwörter an einem sicheren Ort hinterlegt?	N/A
Wenn Passwörter hinterlegt werden: Werden die hinterlegten Passwörter auf dem aktuellen Stand gehalten?	N/A
Wenn Passwörter hinterlegt werden: Wird der Zugriff auf hinterlegte Passwörter dokumentiert?	N/A

Katalognummer: M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile

Das BSI fordert eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?	**Documentation & Reporting** Benutzer- und Gruppenreport
Wird die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile regelmäßig auf Aktualität überprüft?	**Documentation & Reporting** 8MAN aktualisiert die Dokumentation automatisch. Jede in 8MAN vorgenommene Änderung wird erfasst und der jeweiligen Rolle entsprechend automatisiert versendet.
Ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt?	**Documentation & Reporting** 8MAN kann Reporte in geschützte Verzeichnisse und Postfächer exportieren. Die Erstellung der Reporte ist nur durch autorisierte 8MAN Nutzer möglich.

Katalognummer: M 2.65 Kontrolle der Wirksamkeit der Benutzertrennung am IT-System

Nach dem BSI sollte mittels Protokollauswertung oder durch Stichproben überprüft werden, ob Benutzer von IT-Systemen sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wird regelmäßig überprüft, ob alle Benutzer ausschließlich unter ihrer eigenen Kennung arbeiten?	N/A
Sofern Akzeptanzprobleme bezüglich des ordnungsgemäßen Benutzerwechsels bestehen: Werden alternative Maßnahmen untersucht?	N/A

Katalognummer: M 2.402 Zurücksetzen von Passwörtern

Nach dem BSI muss jede Institution für das Zurücksetzen von Passwörtern geeignete Vorgehensweisen definieren.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurde ein für die Organisation angemessenes Verfahren zum Zurücksetzen von Passwörtern definiert?	8MAN löst die Problematik der Mitarbeiteridentifizierung dezentralisiert. Nicht der Help Desk, sondern der direkte Vorgesetzte setzt bei kritischen Nutzerkonten das Passwort zurück. Damit ist „Social Engineering" ausgeschlossen.
Bei höherem Schutzbedarf des Passwortes: Gibt es eine Eskalationsstrategie, falls der Support-Mitarbeiter die Verantwortung nicht übernehmen kann?	
Trägt das festgelegte Verfahren für das Zurücksetzen von Passwörtern dem Schutzbedarf der durch die Passwörter geschützten Ressourcen Rechnung?	Bei unkritischen Nutzerkonten kann die Standardoperation auch an den Help Desk delegiert werden.
Wurden die Support-Mitarbeiter für speziell das Berechtigungsmanagement geschult?	Im Rahmen unserer Professional Services bieten wir auch die Einrichtung und Schulung des Help Desk an.

Katalognummer: M 3.98 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und –mechanismen

Das BSI fordert Institutionen dazu auf, sämtliche Mitarbeiter in den sicheren Umgang mit Authentisierungsverfahren einzuweisen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind alle Mitarbeiter in den korrekten Umgang mit den Authentisierungsverfahren eingewiesen worden?	N/A
Gibt es verständliche Richtlinien für den Umgang mit Authentisierungsverfahren?	N/A
Sind alle Mitarbeiter über die relevanten Regelungen zur Authentisierung informiert?	N/A

Katalognummer: M 4.500 Sicherer Einsatz von Systemen für Identitäts- und Berechtigungsmanagement

Nach dem BSI sollten Systeme für Identitäts- und Berechtigungsmanagement prozessual alle Vorgänge abdecken, die mit dem Anlegen, dem Löschen und dem Ändern von Berechtigungen und Benutzerkennungen zu tun haben.

Dazu gehören:

- Identitätsverwaltung,
- Rollenverwaltung,
-Verwaltung und Pflege von Benutzerkennungen und-berechtigungen: anlegen,
- ändern und löschen
- Richtlinienverwaltung

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind geeignete Werkzeuge für das Identitäts- und Berechtigungsmanagement-System vorhanden?	8MAN hat im Bereich Access Rights Management das größte → Serviceportfolio auf dem Markt. Der gesamte User- Lifecycle lässt sich mit 8MAN abbilden.
Ist das Identitäts- und Berechtigungsmanagement-System ausreichend vor Angriffen geschützt?	8MAN verfügt über eine durch das Active Directory geschützte Authentifizierung. Darüber hinaus verfügt 8MAN über ein Benutzermanagement, in dem sich die einzelnen Anwender klar in ihrem Handlungsradius begrenzen lassen.

Katalognummer: M 6.166 Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System

Das BSI fordert regelmäßige Datensicherungen, damit alle im Identitätsund Berechtigungsmanagement-System gespeicherten Informationen auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Veränderungen weiter verfügbar gemacht werden können.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Werden regelmäßige Datensicherungen der Werkzeuge zum Identitäts- und Berechtigungsmanagement durchgeführt?	Wir empfehlen, die von 8MAN erstellten Scans der Berechtigungssituation (SQL-Datenbank) durch regelmäßige Backups zu schützen.
Gibt es Berechtigungskonzepte für Notfallsituationen?	Sollte ein 8MAN Service ausfallen, greift sofort unsere Watchdog-Funktionalität, die den Dienst erneut startet.
Sind die Notfallberechtigungen beim Ausfall des Identitäts- und Berechtigungsmanagement-Systems noch anwendbar, um die Notfallmaßnahmen umsetzen zu können?	Sollte 8MAN ausfallen, kann jederzeit mit Microsoft Bordmitteln gearbeitet werden.

Katalognummer: M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile

Laut BSI muss eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile vorliegen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?	**Documentation & Reporting** → OU Mitglieder und Gruppenzugehörigkeiten aufzeigen → Wer kann wo über welche Berechtigungsgruppen zugreifen? → Wo haben Benutzer und Gruppen Zugriff? → Wer hat wo Zugriff?
Wird die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile regelmäßig auf Aktualität überprüft?	**Documentation & Reporting** 8MAN erstellt alle Reporte automatisiert und in frei konfigurierbaren Intervallen.
Ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt?	**Documentation & Reporting** Die Reporte lassen sich in geschützten Bereichen speichern oder an ausgesuchte Personenkreise verschicken.
Wird die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile – sofern sie elektronisch erfolgt – in das Datensicherungsverfahren einbezogen?	Wir empfehlen, die von 8MAN erstellten Scans der Berechtigungssituation (SQL-Datenbank) durch regelmäßige Backups zu schützen.

Katalognummer: M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

Das BSI fordert klare Vorgehensweisen beim Ausscheiden von Mitarbeitern.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Sind die Aktivitäten, die beim Weggang oder Funktionswechsel von Mitarbeitern durchzuführen sind, klar geregelt?	**User Provisioning** Mit Hilfe der Profilfunktion kann bei einem Abteilungswechsel eine Führungskraft ihrem Mitarbeiter ein neues Profil zuweisen. Damit werden alte Rechte entzogen und durch einen abteilungsspezifischen Basissatz ersetzt.
Werden die zuständigen Stellen rechtzeitig über das Ausscheiden eines Mitarbeiters unterrichtet?	N/A
Wird sichergestellt, dass sämtliche Zutrittsrechte, Zugangsberechtigungen und Zugriffsrechte einer ausscheidenden Person entzogen und gelöscht werden?	**User Provisioning** Zutrittsrechte lassen sich bei AD administrierten Türsystemen über 8MAN regeln. → Gruppenmitgliedschaften bearbeiten Nutzerkonten können deaktiviert oder inklusive vergebener Berechtigungen gelöscht werden. → Einen Benutzer deaktivieren → Einen Nutzer und seine Berechtigungen löschen
Wird sichergestellt, dass sämtliche institutionseigenen Werte (z. B. Unterlagen, Schlüssel, Rechner, Speichermedien) von einer ausscheidenden Person zurückgefordert und eingezogen werden?	N/A

Katalognummer: M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Auf Systemdateien sollten möglichst nur die Systemadministratoren Zugriff haben.
Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wird der Zugriff auf Systemdateien auf einen möglichst kleinen Kreis von Administratoren beschränkt? Sind Systemverzeichnisse so eingerichtet, dass sie den Benutzern nur die benötigten Privilegien zur Verfügung stellen?	**Permission Analysis** → Ein Verzeichnis und die Berechtigungen darauf identifizieren → Einen Benutzer und seine Berechtigungen identifizieren
Erfolgt die Vergabe von Zugriffsrechten restriktiv und im Einklang mit den organisationseigenen Sicherheitsrichtlinien?	Mit dem 8MAN Profileditor sind Sie in der Lage, Ihre Richtlinien mit Abteilungsprofilen zu verwirklichen.
Wird die Rechtevergabe aller Programme inklusive der von diesen aufgerufenen weiteren Programme überprüft?	N/A
Wird der Zugriff auf Systemdateien immer protokolliert?	**Security Monitoring** → Die Zugriffe auf sensible Dateien ermitteln

Katalognummer: M 4.247 Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista

Nach dem BSI sollte die Sicherheitsgruppe „Jeder" nicht verwendet werden. Die Sicherheitsgruppe „Authentifizierte Benutzer" sollte ebenfalls in keinem der vorinstallierten Dateiordner hinzugefügt werden. Diese Gruppe sollte außerdem aus den Sicherheitseinstellungen des Stammordners entfernt werden.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurden alle Berechtigungen restriktiv nach den so genannten Need-toknow-oder Least-Privilege-Prinzipien vergeben?	**Permission Analysis** → Einen Benutzer und seine Berechtigungen identifizieren
Wurde für Anwendungen unter Windows ein restriktives Berechtigungskonzept definiert und umgesetzt?	N/A
Wurde der Sicherheitsgruppe „Jeder" das Schreibrecht innerhalb von Systemordnern entzogen?	**User Provisioning** → Berechtigungen auf global zugängliche Verzeichnisse im Bulk entfernen
Werden Freigabeberechtigungen nicht an integrierte Systemgruppen wie „Authentifizierte Benutzer" oder „Jeder" erteilt?	**Documentation & Reporting** → Report: Jeder Berechtigungen (im Rich Client) → Report: Authentifizierte Benutzer Berechtigungen (im Rich Client)
Sind die restriktiven Berechtigungen mit dem Patchmanagement und dem Netz- und Systemmanagement abgestimmt?	N/A

Katalognummer: M 4.309 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste

Nach dem BSI ist es notwendig, die Sicherheitsrichtlinie, die Regelungen für die Zugriffsberechtigungen enthält konsequent und konsistent umzusetzen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurden die Zugriffsrechte der Benutzer- und Administratorgruppen gemäß der erstellten Sicherheitsrichtlinie konfiguriert?	N/A
Wurden die sich tatsächlich ergebenden effektiven Rechte auf die Zielobjekte stichprobenartig kontrolliert?	**Permission Analysis** → Ein Verzeichnis und die Berechtigungen darauf identifizieren
Sind die Administratorenrollen und die Delegation von Administrationsrechten konsistent konfiguriert?	**Permission Analysis** → Einen Benutzer und seine Berechtigungen identifizieren **Documentation & Reporting** Kontodetails von Nutzern anzeigen

Katalognummer: M 4.312 Überwachung von Verzeichnisdiensten

Das BSI fordert die kontinuierliche Überwachung der Verzeichnisdienste. Dafür sollten unter anderem die Sicherheitseinstellungen und die Protokolldateien eines Servers regelmäßig überprüft werden. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen.

Zentrale BSI Prüffrage(n)	Wie unterstützt 8MAN?
Wurde ein bedarfsgerechtes Überwachungskonzept für den Verzeichnisdienst entworfen und umgesetzt?	**Security Monitoring** → Änderungen im AD überwachen
Werden wichtige Systemereignisse des Verzeichnisdienstes protokolliert und regelmäßig ausgewertet?	**Security Monitoring** → Temporäre Gruppenmitgliedschaften erkennen → Kennwortzurücksetzungen überwachen → Alarme für AD Gruppen anlegen, bearbeiten und löschen → Alarme für Nutzerkonten anlegen
Werden die Überwachungsparameter des Verzeichnisdienstes im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst?	N/A

8MAN | Protected Networks GmbH

Alt-Moabit 73
10555 Berlin
Germany

T: +49 30 3906345 - 0
E: info@8man.com
W: www.8man.com

Autor:
Fabian Fischer
Teamlead Product Management

T: +49 30 3906345-41
E: fabian@8man.com